Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(7):1-6

Research Article ISSN: 2394 - 658X

Investigating the Security Implications of the Internet of Things (IoT)

Mohammed Mustafa Khan

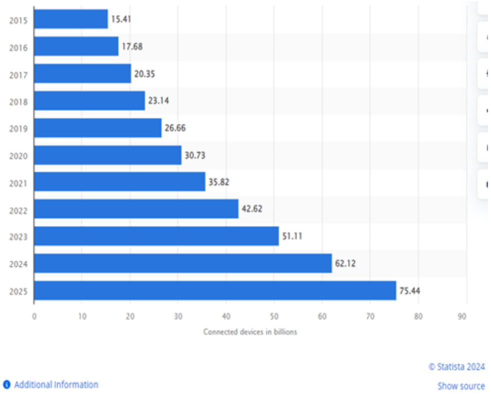
ABSTRACT

In today's hyperconnected world, the Internet of Things (IoT) promises convenience and innovations. The IoT is a game-changing technology paradigm that is changing people's lifestyles and the way they work. The proliferation of smart objects is driven by the rapid advancement of technology. There are various smart objects across different domains, from smart home-based appliances like smart thermostats to industrial machinery and transportation systems. For instance, the manufacturing industry leverages the use of IoT devices like sensors to monitor the performance of machines, discover equipment failures, and enhance production processes. What happens when the IoT appliances/devices designed to help industries turn into nightmare stuff? The security implications of IoT appliances have devastating effects. The security of IoT appliances is weak and is prone to attacks. IoT security is required to protect data breach incidents since IoT appliances do not encrypt their data while in transit over the internet, and their operations can not be detected by standard cybersecurity systems. Many enterprises are grappling with security challenges since IoT appliances were designed with inadequate security capabilities. Additionally, the proliferation and diversity of IoT appliances and communication channels elevate the threat landscape in an organization. Unfortunately, for some IoT devices with low storage and low power, it is nearly impossible to install security software. Moreover, IoT appliances may contain inherent malware and can inject the network once connected. This research paper discusses the security implications of IoT.

Keywords: Security, Smart Objects, IoT products, Data Breach Incidents, Edge Computing, Encryption, Firmware, 5G Network, IoT Architecture, Protocols and Standards.

INTRODUCTION

The IoT is a rapidly evolving technology that has changed the interaction of people in their daily environment. It has enabled industries to collect and share data, control devices, and even remotely manage home and farm plantations with just a click of a button. This technology has been considered one of the most disruptive technologies in the world in the 21st century [2]. The IoT technology comprises different interconnected devices, systems, and sensors that allow the control and monitoring of environments, thus offering a versatile arsenal that enables interactions with our surroundings in unexpected ways. Ahmad & Zhang. (2021) forecast shows that active IoT devices that will be in use will be more than 75 billion in 2025. This will nearly triple the 2019 connected IoT devices, as per the Statista Research Department.



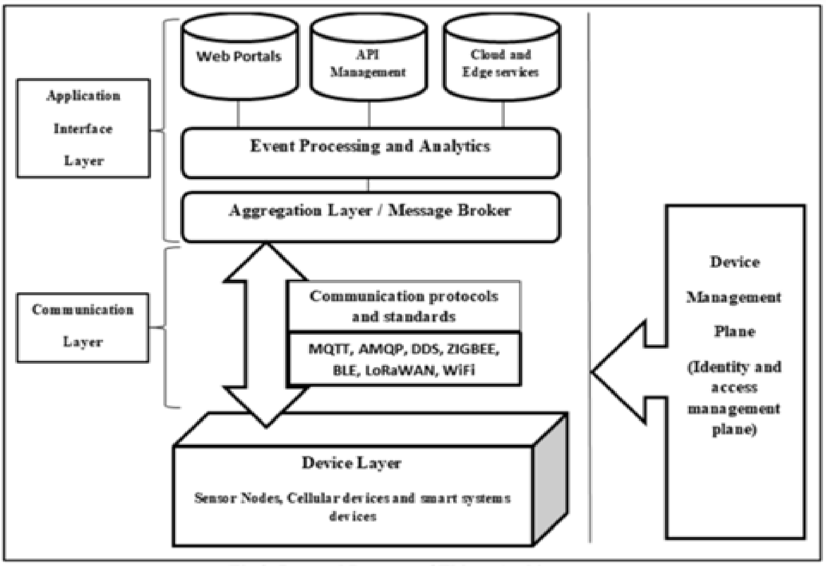
Source: *https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/*

The aspects that drive this growth are automation processes among companies through their digital transformation journey, the impacts of the COVID-19 pandemic that forced people to work remotely, cloud computing technologies, and the rollout of 5G network connectivity, to mention a few. The IoT enables billions of devices, services, and people to connect with others and share information. The rapid rise in the utilization of IoT devices has become an area of interest for cybercriminals, and IoT networks are highly susceptible to security attacks. Advanced security protocols in IoT networks must be deployed to achieve a level of confidentiality, integrity, and availability, among others. According to the 2014 report published by the U.S. Department of Homeland Security (DHS) on the discovered vulnerabilities in the IoT ecosystems, it is imperative for IoT developers and vendors to design IoT devices with security in mind. Intruders can exploit these vulnerabilities, resulting in service disruptions, data breaches, or physical damages.

This paper argues that while IoT offers significant benefits, its rapid adoption without adequate security measures poses severe risks to individual users, industries, and critical infrastructure. By examining the vulnerabilities inherent in IoT devices and the threats they introduce, this paper aims to highlight the importance of implementing powerful security frameworks to protect IoT ecosystems.

IoT ARCHITECTURE

Understanding the technological architecture of IoT devices is the premier foundation in designing and building a secure IoT environment. The IoT contains a multi-plane and multi-layer architecture approach [10]. The architecture can be decomposed into three major sections, including the Application interface, device management plane, and communication plane, as shown below. It is paramount to have a wealth of knowledge in the technological architecture of IoT devices for identifying vulnerabilities, developing tailored security measures, and ensuring superior protection against potential threats.


Web Portals
API Management
Cloud and Edge services
Application Interface Layer
Event Processing and Analytics
Aggregation Layer / Message Broker
Communication Layer
Communication protocols and standards
MQTT, AMQP, DDS, ZIGBEE, BLE, LoRaWAN, WiFi
Device Management Plane (Identity and access management plane)
Device Layer
Sensor Nodes, Cellular devices and smart systems devices

- The application Interface layer enables the interaction of the device with the existing architecture through some embedded interface modules such as sensors, actuators, and Raspberry Pi.
- The device management plane controls the device input and output functionalities by identifying the source and destination of data.
- The communication plane consists of switches and network units that outline the communication protocols like the MQTT (Message Queuing Telemetry Transport) and standards for the IoT network traffic.

CHARACTERISTICS OF IoT

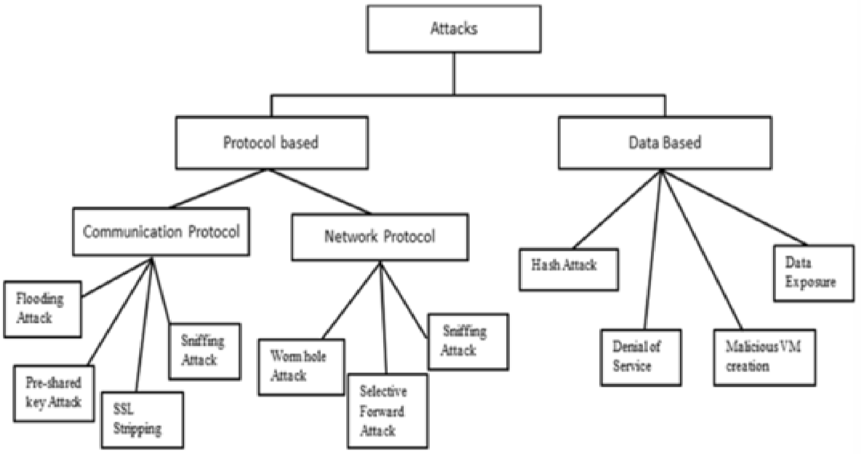
IoT is a collection of devices connected to the internet that collects and shares data using nodes and controllers. IoT devices utilize the controllers and cloud processing capabilities to think and act autonomously and collect information as intended [8]. It is crucial to understand their elements since it helps to tailor security measures to device limitations and ensure effective protection against threats in diverse and resource-constrained environments.

- Completely integrated with or without the need for an operating system (OS) to function.
- Gather real-time data
- Utilizes all types of networks like cellular or Local area Network (LAN)
- Automates decision-making based on the data it collects

- Maintain either constant or occasional cloud connections, necessitating the storage of data with time stamps

CLASSIFICATION OF ATTACKS IN IoT

Intruders focus on two major aspects, including protocol or data, to base their attacks on IoT devices. The protocols and standards used to design and develop IoT tend to be weak and prone to attacks. Additionally, the data transmitted by the IoT devices are encrypted, making it easy to be intercepted by the Man in the middle attack. The types of attacks that are posed by IoT devices can be classified into two major attacks based on the protocol and data, as shown [10].



SECURITY IMPLICATIONS OF THE INTERNET OF THINGS

Weak Authentication and Authorization

IoT devices utilize weak authentication and authorization technologies that can succumb to threats. IoT products are shipped with hard-coded default passwords that cannot be changed. The default credentials like the usernames and passwords are a security threat since extortionist can decrypt the hard-coded passwords using superior cryptographic algorithms and gain access to the information and their communication networks [8]. Hackers can inject malware that can hijack the device to perform botnet attacks.

Lack of Encryption

The size of IoT devices is usually small, with constrained processing memory, power capacities, and resources, making it difficult to encrypt their network traffic. Most IoT devices do not encrypt their data in transit, exposing personal and confidential data that is at risk of cyber threats [10]. For instance, most of the IoT devices used in the healthcare industry to monitor patient health and medical imaging carry very sensitive data about the patient and are encrypted, endangering patient safety.

Vulnerabilities in Firmware and Software

The biggest concerns of IoT devices lie in their application security and endpoint security. The security of IoT devices and applications is poorly designed, making it a honey point for attackers to exploit. The vendors that develop the IoT products must design the products with security in mind [8]. In fact, they must borrow the security, development, and Operations (SecDevOps) framework to guide them in the development of IoT beginning from scratch [9]. The network environment may be jeopardized by vulnerable web applications and IoT device software. Lack of IoT security is the gateway to all risks, whether it is a new threat or conventional malware enabling intruders to launch attacks due to the inherent vulnerabilities in firmware and software.

Insecure Communications Protocols and Channels

IoT refers to a collection of devices that are interlinked together across the internet. An attack on one device can laterally spread the traffic to other devices. IoT devices operate on networks that are not segmented, making it easier to gain access to the target device. For instance, the Valet attack on privacy was experienced by the automotive industries after adopting Bluetooth technology in IoT devices, which led to massive data breach incidents. IoT devices still rely on traditional protocols, such as HTTP and Bluetooth, which are susceptible to attacks [10]. According to the studies carried out by Julio (2018) on automotive vehicles for Tesla Model S that embraced the use of Bluetooth locks technology, hackers were able to unlock the doors, take control of the car, wipe out the speedometer, and were able to shut down the vehicle [1]. This demonstrates the weakness of communication protocols, such as Bluetooth, which are prone to attacks.

Challenges in applying patches and updates to devices

IoT vendors do not focus on embedding IoT security into their devices to harden the hardware, making it tamper-proof for intruders. Many IoT devices have not been developed to support the capabilities of patching or receiving new updates [8]. Once a vulnerability is detected, patches and updates play a vital role in counteracting and rectifying the anomalies. All the identified vulnerabilities can only be stared at, and the intruders can not exploit the loophole. This can not be the case since cyberattacks are happening 24/7.

The Risks of Outdated Technology and Improper Data Disposal

IoT devices are durable in the sense that they have a long shelf life that may go beyond the support of the device. The device becomes outdated, making it difficult to carry out reconfiguration activities or upgrade the firmware when needed. This inability to reconfigure the device is a risk of exposure, and exploiters can capitalize on this vulnerability. Furthermore, a poor data disposal policy without clearing or deleting all the stored data is a security threat when the IoT device gets into the wrong hands [8].

Privacy Issues

The IoT devices have built-in features like cameras, microphones, and night vision. This feature acts as the ears and the eyes of the IoT device. They collect a sheer amount of data without the user's consent. These data can be intercepted by an intruder, compromising the privacy of the user [8]. Failing to disclose data collection, distribution, and usage practices, especially when these are unexpected, can lead to violations of governance and data privacy laws due to lack of transparency.

HOW TO ADDRESS IoT SECURITY REQUIREMENTS?

Risk against organizational assets can be protected by utilizing a conglomeration of multiple layers, including technical, administrative, and physical controls. This forms an organized protection and defense that is tamper-proof to threats and can not be easily broken. Additionally, corporate governance must commit to providing adequate support to cultivate a security structure and culture. IoT security needs a lot of support from the board of directors and executive management.

Proper Designing of IoT Products

The onus is on the vendors and manufacturers to embed security in the design process. They need to check the design principles and fundamentals of security and develop their products from a security standpoint. Application developers, IoT architects, IoT security analysts, and other stakeholders must work in tandem to get the IoT security job done [10]. They ought to embrace the SecDevOps framework approach to ensure that security is introduced in every aspect of development operations [9]. They need to prioritize security as the most integral component of development. Consumers' safety may be at risk if vendors and manufacturers do not rigorously validate the security of their products by testing. The IoT products developed by the manufacturers should ensure they comply with the CIA (Confidentiality, Integrity, and Availability) triad. If manufacturers achieve this CIA triad, they will have hardened the IoT security and protect against most of the common threats.

Segmentation of IoT Products

Segmentation of IoT devices elevates the network security. Segmenting the IoT prevents the spread to other IoT devices in case of a data breach event [8]. The threat can be contained only in a single device. It is fundamental to shut down all the ports that are not in use and deactivate services that are not in use since they act as the gateway avenue for attacks to get into the system. Authentication technology must be incorporated between the devices to ensure data exchange is performed by legitimate objects. The default usernames and passwords must be changed if they can be enabled by the IoT product.

Data Encryption

Data in transit must be encrypted to make it harder for intruders to access the data after even intercepting. The end-to-end communication channels must be secure since attackers are highly trained people who have mastered the architectural design of IoT products, so they know where the weak points exist [10]. The hash integrity checkers can help in the verification process of files or data by generating a hash value based on the content of the file. This hash value serves as a digital fingerprint [8].

Compliance with Regulatory Bodies

Vendors and manufacturers need to comply with specific industry-standard regulatory requirements. Adhering to various regulatory requirements reflects the commitment of manufacturers to fostering IoT security. IoT products developed for healthcare sectors should adhere to the HIPAA (Health Insurance Portability and Policy) Act. Additionally, IoT products developed for European member states should follow the GDPR (General Data Protection Regulation), which governs the collection, sharing, and use of personal data [7]. There are various regulatory requirements that exist. It is the responsibility of the IoT manufacturers to ensure they adhere to the legal laws that exist in different states. Regulation will push manufacturers to consider security factors when designing and developing their products.

Regular Updates and Patches

Routine firmware updates and maintenance are essential for protecting the IoT ecosystem and ensuring its capability to manage all functional operations. It is crucial to have the ability to update firmware, operating systems, or specialized logic on both stationary and mobile IoT devices. This necessitates maintenance interfaces to access the application runtime environment and adjust security settings for the apps on demand. Bugs that have been identified in the IoT products can be rectified by reinforcing the appropriate patch [8]. Providing updates and patching of the IoT product hardens the security capabilities, making it more difficult for cybercriminals to gain access.

Conducting a Risk Assessment for IoT Products

Attackers prey on the negligence of organizations. Organizations that ignore the existence of cyber-attacks are heavily penalized by cybercriminals. Cybercriminals take advantage of organizations that fail to carry out risk assessments of their IoT devices connected to the network [8]. Rogue network devices may be connected on the corporate without the knowledge of Security teams. These devices remain undetected, and they spy on the traffic network as they monitor and transmit traffic to the unauthorized person. Risk assessment will enable the security team to maintain a full inventory of devices connected to their network and disconnect all the rogue devices that are connected to their corporate network. Additionally, risk assessment can help to discover the underlying vulnerabilities and stage corrective measures to seal the loopholes.

Employing Endpoint Security

Deploying endpoint security to monitor network traffic is a tremendous factor in ensuring the security of IoT devices [8]. Monitoring systems like the SIEM (Security Information and Event Management) tool will help to discover any suspicious traffic, and appropriate response is taken as a countermeasure. Additionally, SIEM collects the security information and stores it in a central log file for easy management. It is important for the security teams to manually evaluate these log files to ensure any suspicious logs are attended.

Staff Training

The IBM Security Report on Cyber Resilient Organization indicates that 59% of the respondents say threat sharing enhances the cyber resilience of an organization [5]. The importance of training the staff is to create security awareness so security is staged at the personal level. Advocacy programs that sensitize all stakeholders will help to improve cyber security. Education programs must be conducted regularly to enable threat sharing and maintain the cyber resilience of organizations.

FUTURE TRENDS

Edge Computing

Edge computing is a technology that involves processing and analyzing data close to the source where data is generated [6]. Edge computing eliminates data transfer to another centralized data center or cloud for processing and analysis. Vendors must fully integrate edge computing technology in the IoT products to enhance IoT security by enabling faster, localized, and more efficient protection measures, thereby minimizing vulnerabilities associated with centralized data processing.

CONCLUSION

The application of IoT technology to support business operations begets numerous opportunities and security implications. The security implications of IoT are devastating. It is crucial for organizations to deliberately conduct an assessment of security risk prior to the deployment of IoT devices. This act ensures careful considerations have been put in place regarding the security weak points inherent in the device. Data is the most valuable asset of an organization. It is imperative to ensure IoT products provide maximum data security for them to be sustainable technologies. Therefore, each IoT vendor must ensure they get the IoT architecture right to embed security aspects throughout the design and development stages of the IoT products.

REFERENCE

[1]. J. Poblete, “Dreaming Transnationally in America,” English Language Notes, vol. 56, no. 2, pp. 5–7, Oct. 2018, doi: https://doi.org/10.1215/00138282-6960669.

[2]. J. H. Nord, A. Koohang, and J. Paliszkiewicz, “The Internet of Things: Review and theoretical framework,” Expert Systems with Applications, vol. 133, no. 1, pp. 97–108, Nov. 2019, doi: https://doi.org/10.1016/j.eswa.2019.05.014.

[3]. T. Ahmad and D. Zhang, “Using the internet of things in smart energy systems and networks,” Sustainable Cities and Society, vol. 68, p. 102783, May 2021, doi: https://doi.org/10.1016/j.scs.2021.102783.

[4]. A. T. Chatfield and C. G. Reddick, “A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government,” Government Information Quarterly, vol. 36, no. 2, pp. 346–357, Apr. 2019, doi: https://doi.org/10.1016/j.giq.2018.09.007.

[5]. IBM Security, “Cyber Resilient Organization Report,” 2020. Available: https://riskcue.id/uploads/ebook/20210819081636-2021-08-19ebook081207.pdf

[6]. J. Pan and J. McElhannon, “Future Edge Cloud and Edge Computing for Internet of Things Applications,” IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439–449, Feb. 2018, doi: https://doi.org/10.1109/jiot.2017.2767608.

[7]. P. Renner, “Securing Internet of Things (IoT) Devices that Interact with Personal Information - ProQuest,” Proquest.com, May 2021. https://search.proquest.com/openview/d452c514e35f8d7221f58fb2692f7c16/1?pq-origsite=gscholar&cbl=18750&diss=y

[8]. G. Polat, “Security Issues in IoT: Challenges and Countermeasures,” ISACA, Jan. 02, 2019. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures

[9]. S. D. Duque et al., “Creating It from SCRATCh: A Practical Approach for Enhancing the Security of IoT-Systems in a DevOps-Enabled Software Development Environment,” Lecture Notes in Computer Science, pp. 266–281, Jan. 2020, doi: https://doi.org/10.1007/978-3-030-55583-2_20.

[10]. Rachit, S. Bhatt, and P. R. Ragiri, “Security trends in Internet of Things: a survey,” SN Applied Sciences, vol. 3, no. 1, Jan. 2021, doi: https://doi.org/10.1007/s42452-021-04156-9.